Statement of Work (SOW) for
Ships Navigation & Integrated Bridge System Engineering
Support Services

1.0 INTRODUCTION

1.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Code 522, which is responsible for Ships Navigation & Integration Bridge System (IBS) engineering, installation, testing, repair, and training.

1.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

1.3 Government/Contractor Relationship

1.3.1 The services to be delivered under this Contract are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Contract between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

1.3.2 The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

1.3.3 Contractor personnel under this Contract shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

1.3.4 Employee Relationship:

1.3.4.1 The services to be performed under this Contract do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

1.3.4.2 Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

1.3.2 Inapplicability of Employee Benefits: This Contract does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

1.3.3 Notice: It is the Contractor's, as well as the Government's, responsibility to monitor Contract t activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1.3.3.1 The Contractor shall notify the Contracting Officer in writing via letter or email within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity

of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication involved in the conduct; and the Contractor's estimated date when, absent a response, cost, schedule or performance will be impacted.

1.3.3.2 The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:

(i) Confirm the conduct is in violation and when necessary direct the mode of further performance,

(ii) Countermand any communication regarded as a violation,

(iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or

(iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

1.4 BACKGROUND

The contractor shall provide technical, logistic, program, engineering, training, field engineering (waterfront support and oversight) and administrative support services for the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ECDIS-N and SCS. These services shall include engineering, technical, and programmatic support for the development, testing, and distribution of solutions required to maintain and upgrade designated shipboard ship control systems for the U.S. Navy.

The scope of work shall consist of system design and drawing development, liaison with designated government Life Cycle Managers (LCMs) and In-Service Engineering Agents (ISEAs), and technical services for both new installations and maintenance and repair of legacy systems. The contractor shall support NSWCPD with design, engineering, training, planning, installation, testing, information assurance, integration, and program management support for all work performed under this Contract.

The applicable shipboard systems include the IBS, Integrated Bridge & Navigation Systems (IBNS), SCS, and ECDIS-N. Also applicable are associated support systems such as; I/O units, network switches, servers and firewalls, Ship Control Display System (SCDS), Rudder Angle Display Systems, Shaft RPM Transmitter and Indication systems, Machinery Control Systems (MCS), and monitoring systems.

1.5 SCOPE OF WORK

The contractor shall provide engineering services required for production, testing, evaluation, installation, and life cycle support, as well as the development, implementation, training execution and prototype demonstration for applicable ship control systems. The engineering services include:

- Planning and Program Management Support
- System Design and Integration Engineering
- Test & Evaluation Engineering
- Integrated Logistics Support
- System Installation Support
- Cyber Security Support

The applicable ship control systems include the IBS, IBNS, SCS, Steering & Propulsion Control, ECDIS-N, and associated support equipment.

The associated support equipment includes all items that are part of the above systems and any equipment that directly connects to the boundary of those systems.

2.0 APPLICABLE DOCUMENTS

2.1 Configuration Management Standard EIA649B – [http://standards.sae.org/eia649b/]

2.2 MIL-HDBK-502, DEPARTMENT OF DEFENSE HANDBOOK: ACQUISITION LOGISTICS (30 MAY 1997) – [http://everyspec.com/MIL-HDBK/MIL-HDBK-0500-0599/MIL_HDBK_502_235/]

2.3 MIL-DTL-81927C, DETAIL SPECIFICATION: MANUALS, TECHNICAL: WORK PACKAGE STYLE, FORMAT, AND COMMON TECHNICAL CONTENT REQUIREMENTS; GENERAL SPECIFICATION (NOV 1997) -[http://everyspec.com/MIL-SPECS/MIL-SPECS-MIL-DTL/MIL-DTL-81927C_14024/]

2.4 MIL-STD-38784A (W/ CHANGE-1), DEPARTMENT OF DEFENSE STANDARD PRACTICE: GENERAL STYLE AND FORMAT REQUIREMENTS FOR TECHNICAL MANUALS (11-JUL-2016) - [http://everyspec.com/MIL-STD/MIL-STD-10000-and-Up/MIL-STD-38784A_CHG-1_55081/]

2.5 MIL-DTL-87269D, DETAIL SPECIFICATION: DATA BASE, REVISABLE INTERACTIVE ELECTRONIC TECHNICAL MANUALS, FOR THE SUPPORT OF (30-JAN-2014) - [http://everyspec.com/MIL-SPECS/MIL-SPECS-MIL-DTL/MIL-DTL-87269D_49349/]

2.6 NAVSEA Technical Specification 9090-310G - [http://www.navsea.navy.mil/Portals/103/Documents/NSWC_Dahlgren/FiberOptics/Appendix_H_TS9090-310G_Approved_2015-2-12.pdf]

2.7 DoDD 8500.01x, Information Assurance – [http://www.esd.whs.mil/DD/]

2.8 DoDI 8500.2x, Information Assurance Implementation – [http://www.esd.whs.mil/DD/]

2.9 DODD 8570.01, Information Assurance Training, Certification, and Workforce Management -[http://www.esd.whs.mil/DD/]

2.10 NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010 – [https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf]

2.11 DON CIO Memo 01-09, Information Assurance Policy for Platform Information Technology – [http://www.doncio.navy.mil/policy.aspx]

2.12 NAVSEAINST 9400.2, Implementation of Naval Sea Systems Command (NAVSEA) Afloat Information Assurance (IA) Governance and Guidance – [http://www.navsea.navy.mil/Resources/Instructions/]

2.13 DON-IT Acceptable Use Policy Memorandum, dated 12 FEB 2016. https://www.doncio.navy.mil/Main.aspx

2.14 DON Implementation Of The Risk Management Framework For DoD IT [https://www.doncio.navy.mil/ContentView.aspx?ID=5158]

The Contractor shall reference and utilize the latest version available when performing tasks within this SOW.

3.0. REQUIREMENTS

3.1 Planning and Program Management

3.1.1 The contractor shall provide engineering and technical support to perform the following planning and execution functions for ship control systems on US Navy Ships and Land Based Test Facilities (LBTF). **(CDRL A004)**

3.1.1.1 Assist in the preparation of and participation in program reviews and Configuration Control Board (CCB) meetings conducted by program activities, sponsors and contractors.

3.1.1.2 Provide engineering and maintenance technical services in support of the installation and validation of ship control systems and methodologies.

3.1.1.3 Provide on-site administrative support to Naval Surface Warfare Center Philadelphia Division – Surface Combatants Group. Tasks include travel arrangements, time recording, meeting minutes, records management, financial management, and presentation development.

3.1.1.4 Assist Naval Surface Warfare Center Philadelphia Division – Surface Combatants Group with engineering and technical support, as needed. This will encompass support of ECS/MCS, condition-monitoring systems, platform office support for ship navigation and control systems integration, networks security, and program integration.

3.1.1.5 The contractor will provide both onsite and waterfront engineering support for these services including working group participation, presentation development, and general engineering support.

3.2 System Design & Integration Engineering

3.2.1 The contractor shall assist the Government with the assessment, design, and installation of ship control systems on US Navy Ships and Land Based Test Facilities (LBTF) by supporting system modernization and new concept development. This will include; engineering algorithms, logic trees (as they pertain to systems diagnostics and prognostics), Failure Mode, Effects and Criticality Analysis (FMECA), Expert systems, Verification and validation of software developed to support these new concepts. **(CDRL A005 /CDRL A006)**

3.2.2 The contractor shall perform analysis and technical studies and provide technical services in the area of ship control systems engineering support. The contractor shall provide support to NSWCPD Software Support Activity (SSA) with development, installation, and functional testing of SCS software, including system simulators, and On Board Trainers (OBTs), both shipboard and at LBTFs. **(CDRL A004)**
Areas of particular involvement shall include:

3.2.2.1 Performing investigations and analysis of data, ship plans and ship control systems necessary to develop alteration packages to include SCDs, ECPs, SHIPALTs, and others, as appropriate.

3.2.2.2 Providing engineering support to develop, update, and maintain ship control systems equipment specifications and design documents, and analyzing operational requirements.

3.2.2.3 Engineering support to develop Item Control Drawing (ICD) and Ship Installation Drawing (SID) packages to support ECP and SCD development.

3.2.2.4 Providing system and equipment reliability, maintainability and availability data, and evaluating failure trending and analysis including Failure Mode, Effects and Criticality Analysis (FMECA) and Reliability and Maintainability studies for system components.

3.2.2.5 Reviewing proposed engineering changes for impact on configuration, performance, reliability, maintainability, logistics support, safety, and life cycle costs.

3.2.2.6 Recommending and performing/supporting redesign, modification, or alteration of hardware and software for system integration and improvements.

3.2.2.7 Conducting systems engineering studies for ship control systems.

3.2.2.8 Provide engineering services and technical support to design, develop, and integrate technological improvements into ship control systems.

3.2.2.9 Provide engineering support to develop, update, and maintain ship control system software specifications, design and requirements documentation, including concept papers, interface reviews, preliminary designs, detailed designs, design review participation system and interface requirements, and system and software requirements analysis.

3.2.2.10 Provide engineering support to accomplish ship control systems software deliveries and installations shipboard and at LBTFs or training sites, including software/hardware delivery, audit preparation, and configuration management.

3.3 Test & Evaluation Engineering

3.3.1 The contractor shall provide integration test support for verification of ship control systems integration requirements. In addition, the contractor shall provide validation support for installation and functional testing of ship control systems alterations. Support may also be required for development of Test and Evaluation Master Plans (TEMPs) for installed ship control systems alteration LBTF. **(CDRL A005 /CDRL A006)**

3.3.2 The contractor shall provide test and evaluation support to investigate Ship Control Systems problems and isolate root cause. **(CDRL A004)**

This shall include:

3.3.2.1 Development of test & evaluation plans, including:

3.3.2.1.1 Network Integration Plans

3.3.2.1.2 System Installation Validation

3.3.2.1.3 Verification Plans

3.3.2.1.4 Environmental Testing Plans (Shock, Vibration, Electromagnetic Interference (EMI), ect) as per SOW requirements.

3.3.2.2 Formulate testing methodology and develop test procedures for shipboard and land based SCS.

3.3.2.3 Conduct system integration testing locally and at various testing and integration labs.

3.3.2.4 Develop and perform configuration audits for shipboard systems, LBTFs, and training facilities.

3.3.2.5 Coordinate testing as required for the ISEA with outside activities, commands, and commercial entities as required.

3.3.2.6 Assist the ISEA with providing engineering services for the correction of SCS discrepancies both shipboard and at LBTFs.

3.4 Integrated Logistics Support

3.4.1 The contractor shall provide assistance in development and update of ILS packages, such as; technical manuals/interactive electronic technical manuals (IETMs), training curricula, and other technical data. **(CDRL A005 /CDRL A006)**

3.4.2 Contractor shall support shipping and tracking of material in support of installation and repair efforts.

3.4.3 Contractor shall maintain material for installation and shipboard repair support.

3.5 System Installation Support

3.5.1 The contractor shall provide resources to ISEA in support of equipment installation, training, test, and evaluation of ship control systems. **(CDRL A004/CDRL A005 /CDRL A006)**
This support includes:

3.5.1.1 Assist in the development of installation test procedures, including system operability tests as well as the development and review of installation standards and practices.

3.5.1.2 Making ship visits to design prototype layout plans for ECP / SCD installation, mark up existing installation drawings / documents and capture information for development of new documents.

3.5.1.3 Provide incidental materials such as foundations/ mounting brackets/ cabling/ connectors, and similar type items to support the prototype ship control system installation or other ship control system installations, receipt and stowage of these parts as Government Furnished Equipment (GFE) as required.

3.5.1.4 Provide SCD/SHIPALT/ECD kits (including all hardware and associated documentation) for ship control systems.

3.5.1.5 Conduct shipboard integration testing, verification and validation of signals and troubleshooting of systems.

3.5.1.6 Support development of both operator and maintainer training curriculum.

3.5.1.7 Conduct shipboard and classroom training for operators and maintainers

3.5.1.8 Provide required drawing updates and associated documentation to reflect as built solution and insert as found conditions in the approved SPIR database.

3.5.1.9 Provide on-site support to manage all aspects of material/inventory residing under the cognizance of NSWCPD.

3.5.1.10 Provide on-site support and coordination with item/program managers to ensure material being received and delivered meets program requirements.

3.5.1.11 Provide on-site support to maintain records and controls over material in stock, due in, and planned to ensure accuracy is maintained and material is entered into the government owned database.

3.5.1.12 Provide on-site support to assist or perform yearly audits on 100% of all material in stock to ensure material control is maintained.

3.6 Cyber Security Support (CDRL A004/CDRL A005/CDRL A006)

NSWCPD requires cybersecurity operations support for Shipboards LBTF, and closed-enclave assets. Cybersecurity operations supports includes installation, configuration, and integration of new technology with IT security standards; file backups; security patches; and the performance of analysis to ensure security controls are properly implemented. Operating systems include multiple variants of Unix/Linux, OS X, and Microsoft Windows server and workstation.

The Contractor shall implement configuration version control practices and processes (i.e. checkout/check-in; version number control; system/software baselines; merge, build, test, and release) for software, hardware, firmware, images, technical manuals, test procedures and other support documentation.

3.6.1 Conduct vulnerability assessments of Windows and Linux/UNIX systems, to include:

3.6.2 Vulnerability Scanning & Identification Secure Configuration in accordance with STIG findings.

3.6.3 Ensure Endpoint Compliance – tasks include deployment and management of host-based security products; issuance of antivirus scans, updates, and management/resolution of any discovered issues such as automated software patch distribution and endpoint imaging processing.

3.6.4 Perform intrusion detection analysis and recommend/execute protection against vulnerabilities – tasks include network perimeter Intrusion Detection/Perimeter Security (ID/PS) monitoring, and the adjudication of network-activity; host-based ID/PS monitoring, and the adjudication of host-based activity.

3.6.5 Install security patches on servers to eliminate identified vulnerabilities, and report on patch compliance.

3.6.6 Perform routine audits of systems and software; add, remove, and/or update user account information and perform password-resets, as applicable in accordance with the latest Roster List.

3.6.7 Monitor system-security to maintain security posture, and document the latest version of system-configuration.

3.6.8 Conduct performance tuning – tasks include optimization of equipment and devices to ensure performance of parts and systems is as close to their theoretical peaks as possible.

3.6.9 Research and recommend methods and procedures to implement new security patches and remediation.

3.6.10 Plan and coordinate security measures to safeguard information in computer files against accidental or unauthorized damage, modification or disclosure. Recommendations for implementation shall be presented to NSWCPD.

3.6.11 Plan and support the installation and testing of new products and improvements to computer systems, such as the installation of new databases. Recommendations for implementation shall be presented to NSWCPD. If approved, Contractor shall coordinate and schedule the approved installations.

3.6.12 Develop and prepare implementation-and-maintenance, access control, inventories, and communications-documentation, as well as Standard Operating Procedures (SOPs).

3.6.13 Assist in the preparation of high-level policies and/or strategies for Information Assurance; this includes the development of technical documentation such as:

- 3.6.13.1 Summaries & Whitepapers
- 3.6.13.2 Presentations
- 3.6.13.3 User Manuals
- 3.6.13.4 Administrative Guides

3.6.14 Coordinate and schedule program reviews - Contractor shall maintain master project calendar and coordinate arrangements for presentations/meetings; Contractor shall maintain Plan of Action and Milestones (POAMs)

3.6.15 Assist in the creation and preparation of technical documentation such as user manuals, reports, outlines, and summaries.

3.6.16 Update and manage software libraries in accordance with (SOP) procedures, and execute the destruction of dated versions in accordance with DoD mandates.

3.7 Navy Information Assurance (IA) Workforce Requirements

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, and SECNAV 5239.2, DON IAWF Management Manual to support the Cybersecurity/IAWF Program, contractors performing IA functions must be designated as a member of the Cybersecurity\IA Workforce and meet qualification requirements for their duties, which may include both an IA baseline certification and Operating System (OS)/Computing Environment (CE) certification requirement per below instructions:

3.7.1 Contractors performing Cybersecurity/IA functions must meet the minimum IA baseline certification prior to being engaged as defined in the CSWF Matrix below.

3.7.2 Contractor personnel agree as a "condition of employment" to obtain (and maintain) the appropriate certifications and continuing professional education requirements for their Cybersecurity/IAWF position.

3.7.3 Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570.01M and SECNAV M-5239.2. The contractor is responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570.01M and the Computing Environment/Operating System (CE/OS) certifications in accordance with the CSWF Matrix below.

3.7.4 Upon hire all contractor personnel assigned to the IAM/IAT Level I-III position (as appropriate) shall sign the Information System Privileged Access Agreement and Acknowledgement of Responsibilities statement.

3.8 Cybersecurity/IA Workforce Labor Categories

Cybersecurity/IA Workforce labor categories are identified herein. The Contractor shall ensure that personnel have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including:

3.8.1 DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

3.8.2 Appropriate operating system certification for information assurance technical (IAT) positions as required by DoD 8570.01-M.

3.8.3 The Contractor shall provide the current information assurance certificates/documentation supporting IA certification and current status of personnel performing Cybersecurity/IA duties. Baseline and Operating System (OS) Certification requirements listed in the CSWF Matrix must be met and are a condition of hire.

3.8.4 Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

3.9 Information Assurance Contractor Training & Certification

3.9.1 The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

3.9.1.1 DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

3.9.1.2 Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

3.9.2 Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

3.9.3 Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

3.9.4 After Contract award, the contractor is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.

3.9.5 The responsibilities specified apply to all DoD information assurance duties supported by a contractor, whether performed full-time or part-time as additional or embedded duties, and when using a DoD Contract, or a Contract or agreement administered by another agency.

3.9.6 Baseline Certification- The baseline certification is a security certification and is required for all IA members (all IAT and IAM levels) of the Cybersecurity Workforce/IA

Workforce. Contractors must have a baseline certification prior to performing any IA duties and is a condition of hire.

3.9.7 Computing Environment (CE) Certification- All IAT levels require Computing Environment certification for the appropriate operating system they support and in which access is granted. These certifications are typically vendor specific and depend on the supported hardware or operating system. (i.e., Microsoft computing environment requires MCITP-SA and Linux computing environment requires LINUX+).

4.0 DATA REQUIREMENTS

4.1 Contract Status Report (CDRL A001)

4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.

4.1.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable the Government's approval must be received in writing from the COR within 5 business days before formal submission.

4.2 Travel Report (CDRL A002)

4.2.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.2.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.3 Contractor's Personnel Roster (CDRL A003)

4.3.1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR. This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.4 Technical Report Study/Services (CDRL A004)

4.4.1 Engineering project reports shall be delivered to the SME within fifteen (15) days of completion of the project, the contractor will also provide in process reports as required.

4.5 Key Events Schedule/ Plan Of Action And Milestones (POAM) (CDRL A005)

4.5.1 POA&Ms will be developed and maintained in Microsoft Project software. POA&Ms shall include Calculations, Specifications, Test Data/Reports, and Metrics as required for tasks identified by the TPOC. POA&M's shall be prepared and delivered within 5 working days of identification

4.6 Meeting Minutes (CDRL A006)

4.6.1 Meeting minutes/reports will be generated in Microsoft Word and shall be delivered within 5 working days following meeting completion.

4.7 Government Property Inventory Report (CDRL A007)

4.7.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.7.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.8 Small Business Utilization Report (CDRL A008)

4.8.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.8.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.9 Systems Security Plan CDRL (A009)

4.9.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.9.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.10 CSWF Baseline Certifications (A010)

4.10.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.10.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

Note: Draft technical reports and conclusions reflecting the work accomplished under each task set forth will be prepared and delivered to the Government two (2) weeks before final submittal date and in the form required by the COR. The final report shall not be prepared without approval of the COR. All draft and final reports submitted by the contractor should have computer media attached. All software Programs and databases shall be compatible with government software programs and databases as defined by NMCI.

5.0 SECURITY REQUIREMENTS

5.1 SECURITY TRAINING. The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; NAVSEA Physical Security training and Cybersecurity 101 Training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.2 In accordance with the NISPOM DoD 5220.22M, Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site require an open investigation or favorable adjudicated Tier 3 by the Vetting Risk Operations Center (VROC). An interim clearance is granted by VROC and recorded in the Joint Personnel Adjudication System (JPAS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD buildings. Furthermore, if the Navy Central Adjudication Facility, have made an unfavorable determination access will be denied. For Common Access Card (CAC) you must have an open investigation and or favorable adjusted investigation. Interim security clearance are acceptable for a CAC. Access will be denied for anyone that has eligibility pending in JPAS.

a. Contractor personnel that require a badge to work on-site at NSWCPD must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship.

b. Vetting through the National Crime Information Center, Sex Offender Registry, and the Terrorist screening database shall be process for a contractor that does not have a favorable adjudicated investigation.
Any contractor that has unfavorable information that has not been favorably adjudicated, by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge.

c. Within 30 days after contract award, the contractor shall submit a list of all contractor personnel, including subcontractor employees, who will have access to DON information systems and/or work on-site at one of the NSWCPD sites to the appointed Contracting Officer Representative (COR) via email. The contractor shall provide each employee's first name, last name, contract number, the NSWCPD technical code, work location, whether or not the employee has a CAC and or Standard Access Control Badge (SACB), the systems the employee can access (i.e., NMCI, RDT&E), and the name of the Contractor's local point of contact, phone number and email address. Throughout the period of performance of the

contract, the Contractor shall immediately provide any updated information to the COR when any Contractor personnel changes occur including substitutions or departures.

5.3 ON SITE WORK. Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

5.4 In accordance with NSWCPD security protocol, contractor employees who hold dual citizenship will not be granted security clearance to our facilities.

5.5 This effort may require access to classified information up to the SECRET level. No classified data will be generated or stored by the Contractor. The Contractor is required to have and maintain a SECRET clearance. The requirements of the attached DD Form 254 apply.

5.6 The contractor is required to maintain a Facility Security Clearance (FCL) in accordance with the DD254 to perform certain work under the contract. Although it is not required at time of award, it shall be obtained within 45 days after award. Otherwise the government will have no obligation to continue ordering work under the contract and may not exercise any of the available options.

The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office.

5.7 The Prime Contractor shall:

- 5.7.1 Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.
- 5.7.2 Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.
- 5.7.3 Submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

An Active SECRET Facility Clearance (FCL) is required for performance on this contract. There is no safeguarding requirement required.

All contractor personnel accessing classified information or material associated with and/or performing work relative to the resultant contract must be United States citizens and shall have and maintain at a minimum SECRET security clearance at time of Contract award.

NATO & SIPRnet: This contract does not require access to NATO classified information and there is not a need to know for NATO classified information. Personnel assigned to this contact who require access to SIPRnet and/or SIPRnet Backbone equipment must receive a NATO security briefing and derivative classification training prior to access from the contractor's Facility Security Officer (FSO). The FSO shall ensure all personnel receive an initial and annual NATO security briefing along with initial and biennial derivative classification training during the life of this contract. Evidence of completion, training certificates or equivalent, shall be provided to the Information Assurance Manager no later than the individual's due date. The contractor shall not use the SIPRnet for anything except that which is required for this contract.

NNPI: (U) Security Controls on the Dissemination of NNPI Received or Generated Under NAVSEA Contracts 12/1/2011

Additional information related to the facility clearance process can be obtained by visiting www.dss.mil or http://www.dss.mil/isec/pcl_index.htm.

5.8 The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

5.9 PLANNING, PROGRAMMING, BUDGETING AND EXECUTION (PPBE) DATA. When contractor employees, in the performance of their duties, are exposed to Planning, Programming, Budgeting and Execution (PPBE) data, a Non-Disclosure Agreement (NDA) with all affected contactor personnel must be executed in coordination with the COR and PCO to ensure safeguarding disclosure of this data.

5.9.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews

5.9.1.1 Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

5.9.1.2 If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

5.10 Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

5.11 The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

5.12 Compliance to NIST 800-171

5.12.1 The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

5.12.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

5.12.3 Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

5.12.4 Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

5.12.5 Implement Control 3.1.12 (monitoring and control remote access sessions)- Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

5.12.6 Audit user privileges on at least an annual basis.

5.12.7 Implement:

5.12.7.1 Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

5.12.7.2 NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

5.12.8 Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

5.12.9 Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

5.12.10 Cyber Incident Response:

5.12.10.1 The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the Contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

5.12.10.2 Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

5.12.10.3 If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

5.12.11 Naval Criminal Investigative Service (NCIS) Outreach

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

5.12.13 NCIS/Industry Monitoring

5.12.13.1 In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the

Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

5.12.13.2 If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

5.12.13.4 In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

5.13 U-NNPI SECURITY REQUIREMENTS

5.13.1 Security Classification Guidance is as follows of portions of the tasking on this contract when invoked in the Contract statement of work:

5.13.1.1 Contractor requires access to information and equipment classified at the Confidential National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

5.13.1.2 All contractor personnel accessing classified information or classified material associated with the performance work relative to the resultant contract must be United States citizens no foreign nationals and shall have and maintain at a minimum Confidential security clearance.

5.13.1.3 The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems, as necessary to support.

5.14 U-NNPI

5.14.1. Purpose.

The Contractor hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

5.14.2 Specific Requirements for Protecting U-NNPI

a) Only U.S. citizens who have an NTK required to execute the contract shall be allowed access to U-NNPI.

b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home or automobile, or unattended in a motel room or sent with baggage).

c) U-NNPI documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

d) U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).

e) U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNO (N00N).

f) U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

g) Documents containing U-NNPI shall be disposed of as classified material.

h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

i) Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI.

j) The only approved storage for U-NNPI is CDMS NOFORN.

5.15 OPERATIONS SECURITY (OPSEC)

5.15.1 The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWC Philadelphia Division's (NSWCPD) Critical Information List (CIL)/ CIIL (Critical Indicators and information list) will be provided on site, if warranted. Performance under this contract requires the contractor to adhere to OPSEC requirements. The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements. During the period of this contract, the Contractor may be exposed to, use, or produce, NSWCPD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI).

5.15.2 CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations.
Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible.

5.15.3 NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites. Media requests related to this project shall be directed to the PCO, and the COR who will forward the required to the NSWCPD Public Release Authority for review.

5.15.4 Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWC PD Security Division (Code 105.1). Questions concerning these requirements shall be directed to the PCO, and the COR who will forward the request to the NSWC PD Security Division (Code 105.1).

5.16 RECEIPT, STORAGE, AND GENERATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI) All Controlled Unclassified Information (CUI) associated with this contract must follow the minimum marking requirements of DoDI 5200.48, Section 3, paragraph 3.4.a, and include the acronym "CUI" in the banner and footer of the document. In accordance with DoDI 5200.48, CUI must be safeguarded to prevent Unauthorized Disclosure (UD). CUI export controlled technical information or other scientific, technical, and engineering information must be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. Nonfederal information systems storing and processing CUI shall be protected per NIST SP-800-171, or subsequent revisions. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

6.0 PLACE OF PERFORMANCE

6.1 The contractor's primary place of performance shall be at government facilities in Philadelphia, PA. It is estimated that 88% of the work will occur on-site at the NSWCPD facility and 12% of the work will occur off-site at the contractor facility.

6.1.1 Performance will occur at the following government sites: Naval Surface Warfare Center Philadelphia Division (NSWCPD); 5001 S. Broad St. Philadelphia, PA 19112.

6.1.2 Government will provide office and lab space,
and including computer and phone for up to five (5) Contractor personnel under this Contract. Note NMCI laptops and RDT&E laptops are considered GFP.

6.1.3 The specific location(s) will be provided at time of award of the
Contract. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.4 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a

Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Contract. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

6.1.5 Early Dismissal and Closure of Government Facilities

6.1.5.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

6.1.5.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Contract. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Contract period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

6.1.6 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing performance at NSWCPD. This document is available at: https://navsea.navy.deps.mil/wc/pnbc-code10/Safety/default.aspx

6.1.7 In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by e-mail to Paul Breeden (paul.breeden@navy.mil) that on-site employees have read the "Philadelphia Division Environmental Policy and Commitment" and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD. The e-mail shall include the employee name, work site, and contract number.

6.2 Due to COVID-19, Contractors are encouraged to evaluate and establish performance of its contract at alternate work locations such as the expanded use of teleworking when feasible to successfully perform the contract requirements. This is in effect until there is resolution of the pandemic or as directed by the Contracting Officer.

6.2.1 OCONUS Contractor Personnel Travel During COVID-19

In consideration of personnel movement during the COVID-19 pandemic, Force Health Protection (FHP) guidance has been issued for contractor personnel who travel OCONUS for deployment and for conducting official travel OCONUS as well. Entry requirements are communicated to traveling personnel, including contractor personnel, through the Electronic Foreign Clearance Guide (EFCG). Contractor personnel must adhere to current country entry requirements of the respective geographic combatant command (GCC) (which may include

screening, ROM, and testing) and all applicable host nation procedures. All contracts including performance outside the United States require DoD contractor personnel to complete a risk assessment of health status.

- For each day on NSWCPD property, the contractor shall complete the current version of the NSWCPD COVID-19 Screening and Self-Assessment Questionnaire (Attachment 2) for each employee. If there are any "Yes" answers, the contractor shall contact the TPOC or the Contractor Officer.

7.0 TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated number of trips is 223 per year.

The contractor shall be required to travel CONUS (any state in USA) and OCONUS (primarily Japan, and any country in Europe) to accomplish the tasks contained in this contract. Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations:

CONUS/OCONUS	ORIGIN:	DESTINATION:	Number of Days Per Trip	Number of Trips	Number of People
CONUS	TBD	Marinette, WI	5	5	1
CONUS	TBD	Mobile, AL	5	10	1
CONUS	TBD	Portland, OR	5	5	1
CONUS	TBD	Vigor Ship Yard Seattle, WA	5	10	1
CONUS	TBD	Naval Station, Norfolk, VA	5	19	1
CONUS	TBD	Norfolk Naval Shipyard (NNSY), Portsmouth, VA	5	13	1
CONUS	TBD	Naval Station, Mayport, FL	5	20	1
CONUS	TBD	Naval Station, San Diego, CA	5	30	1
CONUS	TBD	Naval Base, Coronado, CA	5	13	1
CONUS	TBD	Puget Sound Naval Shipyard & Intermediate Maintenance Facility (PSNS&IMF), Bremerton, WA	5	13	1
CONUS	TBD	Naval Station Everett, WA	5	15	1
CONUS	TBD	Naval Base Kitsap, WA	5	15	1
OCONUS	TBD	Ship Repair Facility (SRF) and Combined Fleet Activities (CFAY), Yokosuka, Japan	5	15	1
OCONUS	TBD	SFF Detachment and Combined Fleet Activities Sasebo (CFAS), Japan	5	15	1
OCONUS	TBD	Naval Station Pearl Harbor, HI	5	15	1
OCONUS	TBD	Changi Naval Base, Singapore	5	5	1
OCONUS	TBD	Naval Support Activity Bahrain,	5	5	1

		Bahrain			

7.2 The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved before travel occurs. Approval may be via email by the Contracting Officer (PCO) or the fully executed Technical Instruction (TI) signed by the Contracting Officer.
In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

7.3 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

7.4 **Travel Costs**

7.4.1 The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

7.4.2 The Government shall reimburse the contractor (and its subcontractors) at a reduced reimbursement rate from the current "maximum per diem" rates for lodging, meals, and incidentals, referenced in FAR 31.205-46(a)(2), for any employees, purchased labor, consultants, etc. assigned to a temporary duty station (TDY) in excess of 30 days in one location. This applies to both CONUS and OCONUS travel. The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

7.4.3 When proposed travel is in excess of 30 consecutive days, but less than 180 consecutive days, the Government shall limit reimbursement of contractor (and subcontractor) travel costs, on a flat rate basis, to 75 percent of the per diem rate for the TDY locality at the time of travel (lodging, meals, and incidentals) for each full day, long-term TDY of 31 to 180 days. For travel lasting in excess of 180 days, the Government shall limit reimbursement of contractor (and subcontractor) travel costs, on a flat rate basis, to 55 percent of the per diem rates of the TDY locality at the time of travel for each full day.

8.0 GOVERNMENT FURNISHED PROPERTY

8.1 Government Furnished Material (GFM) will be issued as needed and indicated on each Task Instruction (TI).

8.2 The Government will also authorize access to required government systems such as NMCI and the RDT&E network.

9.0 GOVERNMENT FURNISHED INFORMATION

9.1 Government Furnished Information (GFI) will be issued as needed and indicated on each Task Instruction (TI). The government will provide the contractor with all pertinent information, including deadlines and government propriety data within fourteen (14) working days of request. This government furnished information (GFI) shall be returned to the government within thirty (30) days after completion of this task or with submission of the final report, unless the SME directs that it be destroyed.

10.0 PURCHASES

10.1 Only items directly used and incidental to the services for this Contract and for work within the scope of the Statement of Work, shall be purchased under the Other Direct Cost (ODC) line items. Purchases of an individual item that is valued above $10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

10.2 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Contract shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

11.0 PERSONNEL

11.1 Personnel Requirements. All persons proposed in key and non-key labor categories shall, at the time of proposal submission, be U.S. citizens holding at least a current SECRET clearance, or possess a favorable DCSA adjudication as outlined in section 5.

11.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs.

11.3 The level of effort for the performance of the resultant Contract is based on the labor categories and hours per year as provided in Section B of this Solicitation.

11.4 Key Personnel

11.4.1 The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Contract in accordance with Clause 52.237-3 Continuity of Services (Jan 1991) in the basic SeaPort contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

11.4.2 In accordance with C-237-H002 Substitution of Key Personnel, the following labor categories are designated as the target Key Personnel for this contract. Resumes will be submitted for each category in the quantities indicated by the key category description. Target qualifications are listed below for each education and work experience qualifications for each key personnel labor category. The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for task areas in section 3 in the performance work statement.

11.4.3 The Contractor shall provide individuals to fill the key positions identified below.

11.4.4 The Contractor shall indicate within the personnel section of it's proposal, and/or indicate within individual submitted resume(s), any personnel security clearance requirements as stipulated in section 12.1 above.

Program/Project Manager II (one resume required):

Target Education: Bachelor's level degree in any technical or managerial discipline. In lieu of the education requirement, individuals should have fifteen (15) years of relevant experience in the program management and program oversight of Control System/Information System or other technical equipment, systems or programs for the U.S. Navy.

Target Experience:

- Ten (10) years professional experience in program/project management
- Overall planning, direction and success of major programs, systems development efforts, and research or technology initiatives which have great significance to the activity's and agency's needs
- Establishment and control of technical milestones, schedules, budgets and costs are also essential tasks for the Program Manager
- Working knowledge of the Naval Sea System Command, Naval Surface Warfare Center and Fleet organizations is desired

11.5 Non-Key Personnel

11.5.1 In the performance of this effort, the Contractor shall fully staff the non-key positions listed below with qualified individuals. The Contractor shall provide individuals to fill the non-key positions identified below:

ENGINEER I (E1):
Minimum Education: Bachelor's level degree in an Engineering discipline.
Minimum Experience: No required professional experience.

ENGINEER II (E2)
Minimum Education: Bachelor's level degree in any engineering discipline.
Minimum Experience:

- Three (3) years professional experience in engineering
- One (1) year of professional experience troubleshooting hardware/software systems
- One (1) year of professional experience reading electrical schematics
- One (1) year of professional experience troubleshooting network based systems

ENGINEER III (E3)

Minimum Education: Bachelor's level degree in any engineering discipline.

Minimum Experience:

- Five (5) years professional experience in engineering
- Two (2) years of professional experience within industry acting as a lead engineer
- Three (3) years of professional experience troubleshooting hardware/software systems
- Two (2) years of professional experience reading electrical schematics
- One (1) year of professional experience troubleshooting network based systems

LOGISTICIAN II (LGT2):
Minimum Education: High school/vocational school degree or GED certificate.
Minimum Experience: Seven (7) years of professional experience in integrated logistics support.

CONFIGURATION MANAGEMENT SPECIALIST II (SCM2)
Minimum Education: Bachelor's Degree in Science, Technology, Engineering, or Mathematics.
Minimum Experience:

- Three (3) years of professional experience in configuration management.
- One (1) year of experience with software configuration management specifically as it relates to libraries of multiple software baselines, version control, tracking unique updates to software builds, and conducting diffs of source code
- One (1) year of experience in technical writing
- One (1) year of experience with Waterfall software development life cycle concepts

ELECTRONICS TECHNICIAN, MAINTENANCE (23182)
Minimum Education: High School Diploma or Trade/Industrial School Diploma (or GED Equivalent), or graduate from military schools and/or related military experience.
Minimum Experience:

- Two (2) years of professional/military experience as an Engineering Technician. Experience shall be with Navy equipment and/or machinery on Navy ships and/or land based sites, conducting and witnessing shipboard and/or land based installation and operational testing of U.S. Navy machinery control systems and equipment.
- One year of professional/military experience tracing signals and diagnosing or isolating cause for electrical failures
- One (1) year of professional/military experience reading, understanding, and interpreting electrical schematics
- One (1) year of professional/military experience generating write ups that detail testing performed, troubleshooting steps, and findings
- One (1) year of professional/military experience using a digital multimeter to conduct troubleshooting hardware systems
- One (1) year of professional/military experience using a personal computer to conduct troubleshooting and complete work product tasks

MANAGEMENT ANALYST II (ANM2)
Minimum Education: Bachelor's Degree in a business or technical field.

Minimum Experience: Seven (7) years of experience in engineering/science management, operations research analysis or financial/cost analysis.

ADMINISTRATIVE ASSISTANT (01020):
Minimum Education: High School Diploma (or GED Equivalent)
Minimum Experience: Five (5) years of professional experience in secretarial duties (filing, taking phone calls, scheduling appointments, making travel arrangements)

11.6 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

Each new contract that will require contractors to have privileged access, conduct IT planning, develop/code, or perform cybersecurity/IT functions will include DFARS Clause 252.239-7001 Information Assurance Contractor Training and Certification , and should cite both DoD 8570.01-M "Information Assurance Workforce Improvement Program" and should reference the Cyber Security Workforce (CSWF) Baseline Certifications Report CDRL in Section 4.0 DATA REQUIREMENTS.

11.6.1 The table below outlines the requirements for the listed cyber positions:

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System/Computing Environment (OS/CE) Qualification	IT Level (per SECNAV M-5510.30)
Engineer I	75 - Strategic Planning and Policy Development	Intermediate	IAT-2	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	Directed by the Privileged Access Agreement	IT-II
Engineer II	75 - Strategic Planning and Policy Development	Intermediate	IAT-2	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	Directed by the Privileged Access Agreement	IT-II
Engineer III	75 - Strategic Planning and Policy Development	Expert	IAT-3	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH	Directed by the Privileged Access Agreement	IT-I

12.0 SPECIAL REQUIREMENTS (A007)

12.1 Quality Management System

12.1.1 The Contractor shall:

12.1.1.1 Maintain a Quality Management System (QMS) in accordance with ASQ/ANSI/ISO 9001:2015 standards per Naval Sea Systems Command (NAVSEA) QMS Acceptance Authority or appropriate directorate requirements. All QMS packages are required to adhere to applicable NAVSEA Technical Specification 9090-310 and NAVSEA Standard Item 009-04 requirements.

12.1.1.2 Notify NSWCPD's Quality Department in writing when any changes are made to the QMS that may affect work defined in accordance with NAVSEA Technical Specification 9090-310.

12.1.1.3 Submit its QMS Level 3 specific work procedures relevant to the requirements of the Solicitation, including the SOW at the Contract level (i.e. welding, etc.).

12.2 Risk Management

12.2.1 The contractor shall:

12.2.1.1 Develop an internal risk management program and work jointly with the Code 522 to develop an overall risk management program.

12.2.1.2 Assign responsibility for risk mitigation activities, and monitor progress through a formal tracking system.

12.2.1.3 Conduct risk identification and analysis during all phases of the program, including proposal development. Develop appropriate risk mitigation strategies and plans.

12.2.1.4 Use projected consequences of high probability risks to help establish the level of management reserve and schedule reserve.

12.2.1.5 Assess impact of identified performance, schedule and costs risks to estimate at completion, and include in the estimate as appropriate. Develop a range of estimates (best ase, most likely, worst case).

12.2.1.6 The Contractor shall capture risks and associated mitigation plans in a risk database and provide status updates to the Government for all documented risks upon request.